UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/824,298	04/02/2001	Jeffrey Douglas Haggar	RSW920010036US1	9384

7590 03/19/2007

Jerry W. Herndon
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
MATTIS, JASON E	
ART UNIT	**PAPER NUMBER**
2616	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/824,298	HAGGAR ET AL.	
	Examiner	**Art Unit**	
	Jason E. Mattis	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 20 December 2006.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-10 and 12-47 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-10 and 12-47 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed 12/20/06. Claims 1-10 and 12-47 are currently pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-9, 12, 23-31, 33-43, and 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain et al. (U.S. Pat. 5491801) in view of Firoiu et al. (U.S. pat. 6820128 B1) and Chapman et al. (U.S. Pat. 6643292 B2).

With respect to claims 1, 23, and 35, Jain et al. discloses a method, data processing system, and computer program product with computer code for managing traffic in a network data processing system **(See the abstract of Jain et al. for reference to a method and apparatus for operating a digital communication network to avoid congestion embodied as a process performed by a processor at a station)**. Jain et al. also discloses monitoring traffic for a plurality of network paths **(See column 9 lines 44-55 of Jain et al. for reference to monitoring the throughput**

associated with each source/destination pair sending packets). Jain et al. further discloses prior to sending a packet determining if the packet will cause traffic for the network path to exceed the level of traffic allowed, and if so, reducing the traffic for the network path **(See column 10 line 22 to column 11 line 39 of Jain et al. for reference to identifying packets causing S-D route pairs to have throughputs which are larger than the fair share and before transmitting the packet decreasing the traffic for the violating S-D route pairs by decreasing a window size before more packets are sent).** Jain et al. does not specifically disclose that the traffic for each of the network paths is monitored separately for TCP connections and UDP associations through the network paths and determining if a packet received causes the TCP connection or UDP association to exceed a level of traffic allowed. Jain et al. also does not specifically disclose that the action to reduce bandwidth is based on a transmission protocol corresponding to the one TCP connection or UDP association. Jain et al. further does not disclose that TCP connections or UDP associations that are part of the network path are monitored individually and that the bandwidth for a particular TCP connection or UDP association of the network path is reduced responsive to a packet for the particular TCP connection or UDP association causing the traffic for the network path to exceed a level of traffic allowed.

With respect to claims 7, 29, and 41, Jain et al. discloses a method, data processing system, and computer program product with computer code for managing traffic in a network data processing system **(See the abstract of Jain et al. for reference to a method and apparatus for operating a digital communication**

network to avoid congestion embodied as a process performed by a processor at a station). Jain et al. also discloses monitoring traffic for each of a plurality of network paths **(See column 9 lines 44-55 of Jain et al. for reference to monitoring the throughput associated with each source/destination pair sending packets)**. Jain et al. further discloses prior to sending a packet determining if the packet will cause traffic for the network path to exceed a threshold, and if so, reducing the traffic for the network path **(See column 10 line 22 to column 11 line 39 of Jain et al. for reference to identifying packets causing S-D route pairs to have throughputs which are larger than the fair share, which is a threshold, and before transmitting the packet decreasing the traffic for the violating S-D route pairs by decreasing a window size before more packets are sent)**. Jain et al. does not specifically disclose that the traffic for each of the network paths is monitored separately for TCP connections and UDP associations through the network paths and determining if a packet received causes the TCP connection or UDP association to exceed a level of traffic allowed. Jain et al. also does not specifically disclose that the action to reduce bandwidth is based on a transmission protocol corresponding to the one TCP connection or UDP association. Jain et al. further does not disclose that TCP connections or UDP associations that are part of the network path are monitored individually and that if it is further determined that the packet will cause the traffic for a selected TCP connection or UDP association to exceed its fair share amount of the network path, the traffic for the selected TCP connection or UDP association of the network path is reduced.

With respect to claim 47, Jain et al. does not disclose that the monitoring comprises monitoring at a server the traffic for the plurality of TCP connections or UDP associations.

With respect to claims 1, 7, 23, 29, 35, 41, and 47, Firoiu et al., in the field of communications, discloses a system and method of congestion control wherein traffic is monitored separately for TCP connections and UDP associations and wherein the congestion control action used varies depending on if the traffic is for a TCP connection or a UDP association **(See column 2 line 33 to column 3 line 22, column 1 line 24 to column 2 line 29, column 4 line 15 to column 6 line 15 and Figures 1-2 of Firoiu et al. for reference to a system and method that monitors received traffic to determine if the traffic is for a TCP connection or a UDP association, determines if the traffic received exceeds a current congestion threshold, and takes an action dependent on if the traffic is for a TCP connection or a UDP association to reduce traffic congestion if the congestion threshold has been exceeded)**. Firoiu et al. also discloses that the traffic is monitored at a server **(See column 4 lines 29-41 and Figure 1 of Firoiu et al. for reference to traffic being monitored at network devices 12 that may be servers)**. Using a system and method of congestion control wherein traffic is monitored at a server separately for TCP connections and UDP associations and wherein the congestion control action used varies depending on if the traffic is for a TCP connection or a UDP association has the advantage of allowing the congestion control of packets of each transmission protocol to be treated in the most efficient manner for the particular protocol.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Firoiu et al., to combine using a system and method of congestion control wherein traffic is monitored at a server separately for TCP connections and UDP associations and wherein the congestion control action used varies depending on if the traffic is for a TCP connection or a UDP association, as suggested by Firoiu et al., with the system and method of Jain et al., with the motivation being to allow the congestion control of packets of each transmission protocol to be treated in the most efficient manner for the particular protocol.

With respect to claim 46, Jain et al. does not disclose that if it is further determined that the packet will cause the traffic for a selected TCP connection or UDP association to exceed its fair share amount of the network path, the traffic for the selected TCP connection or UDP association of the network path is reduced.

With respect to claims 1, 7, 23, 29, 35, 41, and 46, Chapman et al., in the field of communications, discloses individually monitoring traffic for particular or selected TCP connections that are a part of a network path and reducing bandwidth available and traffic of a particular or selected TCP connection if it is determined that a packet for the particular or selected TCP connection causing traffic for the particular or selected TCP connection to exceed a threshold level of traffic allowed **(See column 7 line 8 to column 8 line 54 and Figures 7-8 of Chapman et al. for reference to sending data in TCP trunks, which are network paths comprising multiple separate TCP data flows, for reference to setting a minimum bandwidth guarantee for both the entire TCP trunk and for the individual TCP data flows that make up the TCP trunk, for**

reference to monitoring the TCP data flows to determine if the minimum bandwidth guarantee has been met, and for reference to reducing the bandwidth and traffic of a TCP data flow by marking packets of the TCP data flow with a lower priority, meaning more packets are likely to be discarded thus reducing the traffic and bandwidth, if a packet for the TCP data flow causes the TCP data flow to exceed it minimum bandwidth guarantee). Individually monitoring traffic for particular or selected TCP connections that are a part of a network path and reducing bandwidth available and traffic of a particular or selected TCP connection if it is determined that a packet for the particular or selected TCP connection causing traffic for the particular or selected TCP connection to exceed a threshold level of traffic allowed has the advantage of allowing bandwidth allocations of a network path to be controlled separately for each of the connections that make up the network path such that one connection does not cause congestion in another connection by using all the bandwidth allocated to the network path.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Chapman et al., to combine individually monitoring traffic for particular or selected TCP connections that are a part of a network path and reducing bandwidth available and traffic of a particular or selected TCP connection if it is determined that a packet for the particular or selected TCP connection causing traffic for the particular or selected TCP connection to exceed a threshold level of traffic allowed, as suggested by Chapman et al., with the system and method of Jain et al. and Firoiu et al., with the motivation being to allow bandwidth allocations of a

network path to be controlled separately for each of the connections that make up the network path such that one connection does not cause congestion in another connection by using all the bandwidth allocated to the network path.

With respect to claims 2, 8, 24, 30, 36, and 42, Jain et al. discloses that the traffic is monitored using at least one of data transfer rate, peak data transfer rate, burst size, and maximum packet size **(See column 9 line 66 to column 10 line 31 of Jain et al. for reference to measuring throughput, which is the same as data transfer rate).**

With respect to claims 5, 27, 33, 39, and 45, Jain et al. discloses setting and changing a quality of service for packets **(See column 10 lines 22-31 of Jain et al. for reference to setting a congestion avoidance flag, which changes the quality of service of the packet, for packets using on an S-D pair exceeding the fair share).**

With respect to claims 12 and 34, Jain et al. discloses that the threshold takes into account a fair share of bandwidth available for the plurality of network paths **(See column 9 line 44 to column 10 line 31 of Jain et al. for reference to determining the fair share of bandwidth to be allocated to each S-D route pair and using the fair share as a congestion threshold).**

With respect to claims 6, 28, and 40, Jain et al. does not disclose dropping the packet.

With respect to claims 6, 28, and 40, Firoiu et al., in the field of communications discloses dropping a packet in accordance to a rate exceeding a threshold being detected for a particular path **(See column 2 line 33 to column 3 line**

22 of Firoiu et al. for reference to dropping a packet if a rate exceeds a threshold). Dropping a packet has the advantage of quickly reducing the congestion in a network path by not requiring already overused resources to process excess packets when congestion has been detected.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Firoiu et al., to combine dropping a packet, as suggested by Firoiu et al., with the congestion control system and method of Jain et al., with the motivation being to not require already overused resources to process excess packets when congestion has been detected.

4. Claims 3-4, 9, 25-26, 31, 37-38, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain et al. in view Firoiu et al. and Chapman et al. as applied to claims 1-9, 12, 23-31, 33-43, and 45-47 above, and in further view of Qaddoura (U.S. Pat. 6646987).

With respect to claims 3, 9, 25, 31, 37, and 43, Jain et al. discloses reducing a congestion window based on a fair share for a particular network path **(See column 11 line 8-39 of Jain et al. for reference to reducing a window size).** Jain et al. does not disclose that this action takes place when the one TCP connection or UDP association comprises a TCP connection. Although Jain et al. does disclose using a reduction method of multiplying the amount of bandwidth available by a variable chosen as appropriate **(See column 11 line 63 to column 12 line 4)**, the combination of Jain et

al., Firoiu et al., and Chapman et al. does not specifically disclose that the variable is a dynamic variable.

With respect to claims 3, 9, 25, 31, 37, and 43, although Jain et al. does not disclose that this action takes place when the one TCP connection or UDP association comprises a TCP connection, reducing a congestion window size for a TCP connection that has exceeded a level of traffic allowed is old and well known in the art of communications as a method to control TCP connection congestion. Reducing a congestion window size for a TCP connection that has exceeded a level of traffic allowed has the advantage of allowing efficient congestion control for TCP connections to be performed such that congestion is reduced in the system.

It would have been obvious for one of ordinary skill in the art at the time of the invention to combine reducing a congestion window size for a TCP connection that has exceeded a level of traffic allowed with the system and method of Jain et al., Firoiu et al., and Chapman et al. with the motivation being to allow efficient congestion control for TCP connections to be performed such that congestion is reduced in the system.

With respect to claims 4, 26, and 38, Jain et al. discloses reducing the congestion window using an equation CW = max(MinW, min(CW*F,MaxW)). Jain et al. discloses that a window size is reduced by a fraction of 0.875 times the current window size according to rules limiting a window size to a maximum and a minimum window size, which performs the same function as the claimed equation **(See column 11 lines 8-62 of Jain et al. for reference to the rules for reducing the window size).** Although Jain et al. does disclose using a fraction, c, chosen as appropriate **(See**

column 11 line 63 to column 12 line 4), the combination of Jain et al., Firoiu et al., and Chapman et al. does not specifically disclose that the fraction is a dynamic variable.

With respect to claims 3-4, 9, 25-26, 31, 37-38, and 43, Qaddoura, in the field of communications, discloses adjusting a congestion window size using a dynamic variable **(See column 6 lines 42-52 of Qaddoura for reference to automatically adjusting a congestion window size to be a variable of a maximum congestion window size)**. Using a dynamic variable to adjust a congestion window size has the advantage of providing greater control over the amount of congestion window size reduction.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Qaddoura, to combine using a dynamic variable to adjust a congestion window size, as suggested by Qaddoura, with the system and method of Jain et al., Firoiu et al., and Chapman et al., with the motivation being to provide greater control over the amount of congestion window size reduction.

5. Claims 10, 32, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain et al. in view Firoiu et al. and Chapman et al. as applied to claims 1-9, 12, 23-31, 33-43, and 45-47 above, and in further view of Blasbalg (U.S. Pat. 4771391).

With respect to claims 10, 32, and 44, the combination of Jain et al., Firoiu et al., and Chapman et al. does not disclose reducing a sending size for data packets.

With respect to claims 10, 32, and 44, Blasbalg, in the field of communications, discloses reducing the sending size of data packets when congestion is detected **(See column 12 line 53 to column 13 line 9 of Blasbalg for reference to reducing the packet size of packets on a congested path)**. Reducing the sending size of packets has the advantage of providing a way of reducing congestion on a path while still allowing some traffic to pass on the path.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Blasbalg, to combine reducing the sending size of packets, as suggested by Blasbalg, with the congestion control system and method of Jain et al., Firoiu et al., and Chapman et al., with the motivation being to provide a way of reducing congestion on a path while still allowing some traffic to pass on the path.

6. Claims 13-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Packer et al. (U.S. Pat. 6205120) in view of Jain et al., Firoiu et al., and Chapman et al.

With respect to claims 13 and 18, Packer et al. discloses a data processing system **(See column 4 lines 29-44 and Figure 1A of Packer et al. for reference to a client-server computer system, which is a data processing system)**. Packer et al. also discloses a bus system **(See column 4 lines 45-59 and Figure 1A of Packer et al. for reference to bus subsystem 32)**. Packer et al. further discloses a communications unit connected to the bus **(See column 4 lines 45-59 and Figure 1A of Packer et al. for reference to a network interface 40, which is a**

communications unit, connected to bus subsystem 32). Packer et al. also discloses a memory connected to the bus system **(See column 4 lines 45-59 and Figure 1A of Packer et al. for reference to storage subsystem 35 connected to bus subsystem 32)**. Packer et al. further discloses a processor unit connected to the bus system **(See column 4 lines 45-59 and Figure 1A of Packer et al. for reference to processor 30 connected to bus subsystem 32)**. Although the system or Packer et al. discloses implementing congestion control, Packer et al. does not specifically disclose monitoring traffic for a plurality of network paths and reducing an amount of bandwidth available to a particular network path using an action based on a protocol used by the particular network path in response to a packet for a particular network path causing traffic to exceed a level of traffic allowed, wherein the action varies for different transmission protocols.

With respect to claims 13 and 18, Jain et al., in the field of communications, discloses monitoring traffic for a plurality of network paths **(See column 9 lines 44-55 of Jain et al. for reference to monitoring the throughput associated with each source/destination pair sending packets)**. Jain et al. further discloses prior to sending a packet determining if the packet will cause traffic for the network path to exceed a threshold, and if so, reducing the traffic for the network path **(See column 10 line 22 to column 11 line 39 of Jain et al. for reference to identifying packets causing S-D route pairs to have throughputs which are larger than the fair share, which is a threshold, and before transmitting the packet decreasing the traffic for the violating S-D route pairs by decreasing a window size before more packets**

are sent). Monitoring traffic for a plurality of network paths and reducing an amount of bandwidth available based on a fair share for the particular network path in response to a packet for a particular network path causing traffic to exceed a level of traffic allowed has the advantage of providing a congestion control method to stop overused data paths from flooding network resources.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Jain et al., to combine monitoring traffic for a plurality of network paths and reducing an amount of bandwidth available based on a fair share for the particular network path in response to a packet for a particular network path causing traffic to exceed a level of traffic allowed, as suggested by Jain et al., with the data processing system of Packer et al., with the motivation being to provide a congestion control method to stop overused data paths from flooding network resources.

With respect to claims 13 and 18, the combination of Packer et al. and Jain et al. does not specifically disclose that the traffic for each of the network paths is monitored separately for TCP connections and UDP associations through the network paths and determining if a packet received causes one the TCP connections or UDP associations to exceed a level of traffic allowed. The combination of Packer et al. and Jain et al. also does not specifically disclose that the action to reduce bandwidth is based on a transmission protocol corresponding to the one TCP connection or UDP association.

With respect to claims 13 and 18, Firoiu et al., in the field of communications, discloses a system and method of congestion control wherein traffic is monitored separately for TCP connections and UDP associations and wherein the congestion control action used varies depending on if the traffic is for a TCP connection or a UDP association **(See column 2 line 33 to column 3 line 22, column 1 line 24 to column 2 line 29, column 4 line 15 to column 6 line 15 and Figures 1-2 of Firoiu et al. for reference to a system and method that monitors received traffic to determine if the traffic is for a TCP connection or a UDP association, determines if the traffic received exceeds a current congestion threshold, and takes an action dependent on if the traffic is for a TCP connection or a UDP association to reduce traffic congestion if the congestion threshold has been exceeded)**. Using a system and method of congestion control wherein traffic is monitored separately for TCP connections and UDP associations and wherein the congestion control action used varies depending on if the traffic is for a TCP connection or a UDP association has the advantage of allowing the congestion control of packets of each transmission protocol to be treated in the most efficient manner for the particular protocol.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Firoiu et al., to combine using a system and method of congestion control wherein traffic is monitored separately for TCP connections and UDP associations and wherein the congestion control action used varies depending on if the traffic is for a TCP connection or a UDP association, as suggested by Firoiu et al., with the system and method of Packer et al. and Jain et al.,

with the motivation being to allow the congestion control of packets of each transmission protocol to be treated in the most efficient manner for the particular protocol.

With respect to claims 13 and 18, the combination of Packer et al. and Jain et al. further does not disclose that TCP connections or UDP associations that are part of the network path are monitored individually and that if it is further determined that the packet will cause the traffic for a selected TCP connection or UDP association to exceed its fair share amount of the network path, the traffic for the selected TCP connection or UDP association of the network path is reduced.

With respect to claims 13 and 18, Chapman et al., in the field of communications, discloses individually monitoring traffic for particular or selected TCP connections that are a part of a network path and reducing bandwidth available and traffic of a particular or selected TCP connection if it is determined that a packet for the particular or selected TCP connection causing traffic for the particular or selected TCP connection to exceed a threshold level of traffic allowed **(See column 7 line 8 to column 8 line 54 and Figures 7-8 of Chapman et al. for reference to sending data in TCP trunks, which are network paths comprising multiple separate TCP data flows, for reference to setting a minimum bandwidth guarantee for both the entire TCP trunk and for the individual TCP data flows that make up the TCP trunk, for reference to monitoring the TCP data flows to determine if the minimum bandwidth guarantee has been met, and for reference to reducing the bandwidth and traffic of a TCP data flow by marking packets of the TCP data flow with a**

lower priority, meaning more packets are likely to be discarded thus reducing the traffic and bandwidth, if a packet for the TCP data flow causes the TCP data flow to exceed it minimum bandwidth guarantee). Individually monitoring traffic for particular or selected TCP connections that are a part of a network path and reducing bandwidth available and traffic of a particular or selected TCP connection if it is determined that a packet for the particular or selected TCP connection causing traffic for the particular or selected TCP connection to exceed a threshold level of traffic allowed has the advantage of allowing bandwidth allocations of a network path to be controlled separately for each of the connections that make up the network path such that one connection does not cause congestion in another connection by using all the bandwidth allocated to the network path.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Chapman et al., to combine individually monitoring traffic for particular or selected TCP connections that are a part of a network path and reducing bandwidth available and traffic of a particular or selected TCP connection if it is determined that a packet for the particular or selected TCP connection causing traffic for the particular or selected TCP connection to exceed a threshold level of traffic allowed, as suggested by Chapman et al., with the system and method of Jain et al. and Firoiu et al., with the motivation being to allow bandwidth allocations of a network path to be controlled separately for each of the connections that make up the network path such that one connection does not cause congestion in another connection by using all the bandwidth allocated to the network path.

With respect to claims 14 and 19, Packer et al. discloses a primary bus and a secondary bus **(See column 5 lines 1-8 of Packer et al. for reference to using multiple busses, which would include a primary bus and secondary busses).**

With respect to claims 15 and 20, Packer et al. discloses using a single processor **(See column 4 lines 45-59 and Figure 1A of Packer et al. for reference to using one or more processors 30).**

With respect to claims 16 and 21, Packer et al. discloses that the processor unit includes a plurality of processors **(See column 4 lines 45-59 and Figure 1A of Packer et al. for reference to using one or more processors 30).**

With respect to claims 17 and 22, Packer et al. discloses that the communications unit is an Ethernet adapter **(See column 4 lines 45-59 and Figure 1A of Packer et al. for reference to the network interface block 40 employing Ethernet).**

Response to Arguments

7. Applicant's arguments with respect to claims 1-10 and 12-47 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason E. Mattis whose telephone number is (571) 272-3154. The examiner can normally be reached on M-F 8AM-5:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

jem

HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600